# 楕円曲線暗号の攻撃とその安全性 (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

安田, 雅哉

CITATION:

安田, 雅哉. 楕円曲線暗号の攻撃とその安全性 (Computer Algebra : Design of Algorithms, Implementations and Applications). 数理解析研究所講究録 2012, 1814: 74-84

ISSUE DATE:

2012-10

URL:

http://hdl.handle.net/2433/194549

数理解析研究所講究録
第1814巻 2012年 74-84



# 楕円曲線暗号の攻撃とその安全性

安田　雅哉（富士通研究所）

## 1　はじめに

楕円曲線暗号とは、1985年にKoblitz氏とMiller氏がほぼ同時期に独立に考案した暗号であり、楕円曲線と呼ばれる数式によって定義される特殊な加算法に基づいて暗号化・復号化を行う暗号方式である。楕円曲線暗号の解読の困難さは、楕円曲線離散対数問題と呼ばれる問題を解くのと同程度と言われ、一部の曲線を除き効率の良い攻撃法はまだ発見されていない。ここでは、楕円曲線離散対数問題に対する攻撃法を紹介し、その攻撃法に対する楕円曲線暗号の安全性を説明する。

## 2　楕円曲線と楕円曲線離散対数問題

### 2.1　楕円曲線と加算

$p>3$を素数とし、有限体$\mathbb{F}_p$上の楕円曲線

$$E: y^2 = x^3 + ax + b \quad (a, b \in \mathbb{F}_p)$$

を考える。楕円曲線の点の集合全体は以下で定義する加法について群をなすことが知られている（ただし、無限遠点$O$も楕円曲線の点とみなす）：

(i) $P + O = O + P = P$.

(ii) $P = (x, y)$に対し、$-P = (x, -y)$.

(iii) $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$に対し、$P_1 + P_2 = (x_3, y_3)$とする。$P_1 \neq \pm P_2$のとき、

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \\ y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \end{cases}$$

(iv) $P = (x_1, y_1)$に対し、$2P = (x_3, y_3)$とする。$P \neq -P$のとき、

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1, \\ y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1. \end{cases}$$

例 (楕円曲線の点). 有限体 $\mathbb{F}_7$ 上の楕円曲線 $E : y^2 = x^3 + 3x + 4$ の点 $P_1 = (0, 2)$ に対して、$P_n = nP_1$ とおく。このとき、$P_n$ は以下のようになる：

| | | | | |
|---|---|---|---|---|
| $P_1 = (0, 2)$ | $P_2 = (1, 1)$ | $P_3 = (2, 2)$ | $P_4 = (5, 2)$ | $P_5 = (6, 0)$ |
| $P_6 = (5, 5)$ | $P_7 = (2, 5)$ | $P_8 = (1, 6)$ | $P_9 = (0, 5)$ | $P_{10} = O$ |

## 2.2 楕円曲線離散対数問題（ECDLP）

楕円曲線暗号の安全性に深く関わる問題である楕円曲線離散対数問題とは以下の問題である。また、楕円曲線離散対数問題を ECDLP(Elliptic Curve Discrete Logarithm Problem) と略すことが多い。

楕円曲線離散対数問題（ECDLP）

$p > 3$ を素数とし、有限体 $\mathbb{F}_p$ 上の楕円曲線

$$E : y^2 = x^3 + ax + b$$

を考える。素数位数 $r$ の楕円曲線の点 $S = (x_S, y_S)$ を固定し、$T = (x_T, y_T) \in \langle S \rangle$ とする。このとき、$T = dS$ を満たす整数 $d$ を見つけよ。

以下では、上記の記号を用いることにする。

楕円曲線の点 $S$ を固定したとき、

- 整数 $d$ から楕円曲線の点 $T = dS$ は容易に計算可能である。(約 $\log(r)$-回の楕円曲線演算を行えば求まる。)
- $S$ と $T$ から $T = dS$ を満たす整数 $d$ を見つけることは困難である。(素数 $p$ の大きさを 160 ビット程度に選べば、現在最も効率のよいアルゴリズムを用い、最新のコンピュータで計算しても現実的な時間では解は求まらない。)

この性質を用いて構成されるのが楕円曲線暗号である。

例 (ECDLP の数値例). ECDLP の数値例については、カナダの Certicom 社による 1997 年に始まった ECC challenge が有名である。以下で、ECC challenge 問題をいくつか紹介しておく [2]：

(i) ECCp-79（ECC challengeの中で最も簡単）

$$\begin{cases} p = 62CE5177412ACA899CF5 \\ a = 39C95E6DDDB1BC45733C \\ b = 1F16D880E89D5A1C0ED1 \\ r = 1CE4AF36EED8DE22B99D \\ x_S = 315D4B201C208475057D \\ y_S = 035F3DF5AB370252450A \\ x_T = 0679834CEFB7215DC365 \\ y_T = 4084BC50388C4E6FDFAB \end{cases}$$

(ii) ECCp-163 (楕円曲線暗号で通常使用されるパラメータサイズ)

$$\begin{cases} p = 05177B8A2A0FD6A4FF55CDA06B0924E125F86CAD9B \\ a = 043182D283FCE3880730C9A2FDD3F6016529A166AF \\ b = 020C61E9459E53D8871BCAADC2DFC8AD5225228035 \\ r = 003FEA47B8B292641C57F9BF84BAECDE8BB3ADCE30 \\ x_S = 0017E7012277E1B4E43F7BF74657E8BE08BACA175B \\ y_S = 00AA03A0A82690704697E8C504CB135B2B6EEF3C83 \\ x_T = 01DC1E9A482085B3DFA722EB7A541D50505ED31DCA \\ y_T = 012D71ECC1578BFBE203D0C2CE238EB6060ADCAA1E \end{cases}$$

ちなみに、ECCp-**の**はビットサイズを表し、各値は16進数で表記している。

# 3 ECDLPに対する攻撃

ここでは、3つのECDLPに対する攻撃法について説明する。

## 3.1 MOV攻撃

1990年にMenezes, 岡本及びVanstoneによって提案され、Frey-Rückによって拡張された攻撃法 [5]。ECDLPを乗法群の離散対数問題（DLP）に帰着させる。

楕円曲線 $E$ の部分群 $E[r] = \{Q \in E(\overline{\mathbb{F}}_p) \mid rQ = O\}$ を考える。整数 $m$ を $r \mid p^m - 1$ かつ $E[r] \subset E(\mathbb{F}_{p^m})$ となる最小のものとする。しかし、これは以下の補題より $r \nmid p-1$ のとき $r \mid p^m - 1$ の条件だけで十分である。

**補題 3.1.** 素数 $r$ が $r \mid \sharp E(\mathbb{F}_p)$ かつ $r \nmid p-1$ とする。このとき、任意の整数 $m$ に対して以下が成り立つ：

$$E[r] \subset E(\mathbb{F}_{p^m}) \Leftrightarrow r \mid p^m - 1.$$

$G = \mathrm{Gal}\,(\overline{\mathbb{F}}_p/\mathbb{F}_{p^m})$ とおく。$G$-加群の短完全系列

$$0 \to E[r] \to E(\overline{\mathbb{F}}_p) \xrightarrow{r} E(\overline{\mathbb{F}}_p) \to 0$$

を考える。ガロアコホモロジーを考えることにより、長完全系列

$$\begin{aligned} 0 \;\to\; & E[r]^G \;\to\; E(\mathbb{F}_{p^m}) \xrightarrow{r} E(\mathbb{F}_{p^m}) \\ \xrightarrow{\delta}\; & H^1(G, E[r]) \;\to\; H^1(G, E(\overline{\mathbb{F}}_p)) \xrightarrow{r} H^1(G, E(\overline{F}_p)) \;\to \cdots \end{aligned}$$

が得られる。これより、単射準同型

$$\delta_E : E(\mathbb{F}_{p^m})/rE(\mathbb{F}_{p^m}) \to H^1(G, E[r]) = \mathrm{Hom}(G, E[r])$$

が得られる。ただし、$\delta_E(P) = [G \ni \sigma \mapsto \sigma(Q) - Q \in E[r]]$ とする（$P = rQ$ なる $Q$ を固定）。単射準同型 $\delta_E$ と Weil pairing $e_r : E[r] \times E[r] \to \mu_r$ を組み合わせて、次の双線形写像が得られる：

$$\kappa : E(\mathbb{F}_{p^m})/rE(\mathbb{F}_{p^m}) \times E[r] \to \mathrm{Hom}(G, \mu_r) \simeq \mathbb{F}_{p^m}^{\times}/(\mathbb{F}_{p^m}^{\times})^r.$$

ただし、$\mu_r = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^r = 1\}$ とし $\kappa(P, Q) = [G \ni \sigma \mapsto e_r(\delta_E(P)(\sigma), Q) \in \mathrm{Hom}(G, \mu_r)]$ とおく。双線形写像 $\kappa$ について、以下のことが知られている：

- $\kappa$ は非退化。
- $\kappa$ は効率的に計算可能（Miller アルゴリズム）。

次に ECDLP に対する MOV 攻撃アルゴリズムを以下に示す：

**Algorithm 1** MOV 攻撃

**Require:** 素数位数 $r$ の点 $S \in E(\mathbb{F}_p)$, $T \in \langle S \rangle$.
**Ensure:** $T = dS$ を満たす整数 $d$.

1: $E[r] \subset E(\mathbb{F}_{p^m})$ を満たす整数 $m$ を見つける。
2: $\kappa(P, S) \neq 1$ を満たす $P \in E(\mathbb{F}_{p^m})$ を見つける。
3: $\zeta_1 \leftarrow \kappa(P, S)$.
4: $\zeta_2 \leftarrow \kappa(P, T)$.
5: 群 $\mathbb{F}_{p^m}^{\times}$ において $\zeta_1^d = \zeta_2$ となる整数 $d$ を見つける。
6: 整数 $d$ を出力。

注 3.2. MOV 攻撃アルゴリズムのステップ 5 において、$m$ の値が大きい場合は群 $\mathbb{F}_{p^m}^{\times}$ において $\zeta_1^d = \zeta_2$ となる整数 $d$ を見つけることは困難である。ゆえに $m$ が十分小さいとき、MOV 攻撃は有効だとされている。特に、$E$ が supersingular 楕円曲線のとき $m = 2$ であるので、supersingular 楕円曲線に対して MOV 攻撃は有効である。また、整数 $m$ のことを**埋め込み次数**と呼ぶことがある。

## 3.2 SSSA 攻撃

1997 年に Smart-Semaev、佐藤-荒木らにより独立に提案された攻撃法 [6]。Anomalous 楕円曲線のときのみ有効。

定義 (ANOMALOUS 楕円曲線). 有限体 $\mathbb{F}_p$ 上の楕円曲線 $E$ の位数 $\sharp E(\mathbb{F}_p)$ が丁度 $p$ となるとき、楕円曲線 $E$ を **anomalous** と呼ぶ。

有限体 $\mathbb{F}_p$ 上の楕円曲線 $E$ の方程式の各係数を $p$-進数体 $\mathbb{Q}_p$ に持ち上げて、$\mathbb{Q}_p$ 上の楕円曲線 $\widetilde{E}$ を構成する。このとき、短完全列

$$0 \to \ker \pi \to \widetilde{E}(\mathbb{Q}_p) \xrightarrow{\pi} E(\mathbb{F}_p) \to 0$$

が存在する。ただし、$\pi$ は還元写像とする。また、$\mathcal{E}$ を $\widetilde{E}$ に付随する形式群としたとき、対応 $(x, y) \mapsto -x/y$ で定まる同型

$$\ker \pi \simeq \mathcal{E}(p\mathbb{Z}_p) = p\mathbb{Z}_p$$

が存在することが知られている。任意の持ち上げ写像 $u : E(\mathbb{F}_p) \to \widetilde{E}(\mathbb{Q}_p)$ に対して、以下の合成写像を考える：

$$\lambda(u) : E(\mathbb{F}_p) \xrightarrow{u} \widetilde{E}(\mathbb{Q}_p) \xrightarrow{N} \ker \pi \simeq \mathcal{E}(p\mathbb{Z}_p) = p\mathbb{Z}_p \xrightarrow{\bmod p^2} p\mathbb{Z}_p/p^2\mathbb{Z}_p = \mathbb{F}_p$$

ただし、$N = \sharp E(\mathbb{F}_p)$ とする。このとき以下が成り立つ：

**命題 3.3.** $N = p$（楕円曲線 $E$ が anomalous）のとき、任意の持ち上げ写像 $u$ に対して定まる写像 $\lambda(u)$ は同型写像か零写像である。

次に ECDLP に対する SSSA 攻撃アルゴリズムを以下に示す：

---

**Algorithm 2** SSSA 攻撃アルゴリズム

---

**Require:** 素数位数 $r = p$ の点 $S \in E(\mathbb{F}_p), T \in \langle S \rangle$（ただし、$E$ は anomalous）。
**Ensure:** $T = dS$ を満たす整数 $d$.

1: 写像 $\lambda(u)$ が同型となる持ち上げ写像 $u$ を固定。
2: $s \leftarrow \lambda(u)(S)$.
3: $t \leftarrow \lambda(u)(T)$.
4: 群 $\mathbb{F}_p$ において $t = ds$ となる整数 $d$ を見つける。
5: 整数 $d$ を出力。

---

注 3.4. SSSA 攻撃アルゴリズムは、素数 $p$ に対する多項式時間で計算可能。

## 3.3 ρ法攻撃

1978年にPollardによって提案された一般のDLPに対する攻撃法[4]。現在、一般の楕円曲線離散対数問題に対して最も効率がよい。ただし、一般の楕円曲線離散対数問題とは先に紹介したMOV攻撃とSSSA攻撃に対し有効でないものとする。

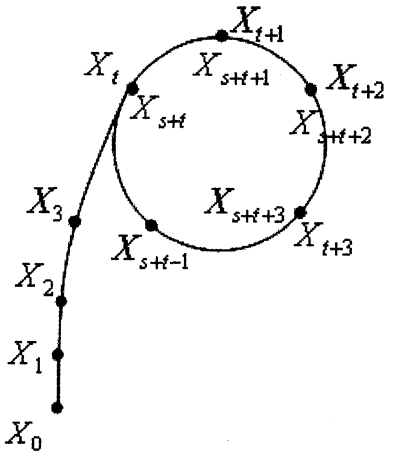
ECDLPから得られる組$(E, S, T)$に対して、写像$f : \langle S\rangle \to \langle S\rangle$を

$$f(X) = X + aS + bT$$

となる整数$a, b$が容易に計算できるものとする。初期点$X_0 = u_0S + v_0T \in E(\mathbb{F}_p)$とおき、

$$X_{i+1} = f(X_i) \quad (i = 0, 1, 2, \cdots)$$

とおく。このとき、写像$f$の選び方から$X_i = u_iS + v_iT$を満たす整数$u_i, v_i$が計算できる。群$\langle S\rangle$は位数$r$の有限集合だから、点$X_i$を順に計算していくと、やがて既に得られた点と等しくなる（**衝突**と呼ぶ）。点$X_{s+t}$がはじめて既に得られた点$X_t$と等しくなったとすると、以下の図のようになる：




衝突した点$X_i = X_j$ $(i \neq j)$を考えると、関係式

$$u_iS + v_iT = u_jS + v_jT$$

が成り立つ。これより、$v_i \not\equiv v_j \pmod r$のとき

$$d = \frac{u_i - u_j}{v_j - v_i} \pmod r$$

となる整数$d$を一つ固定すると、$T = dS$となりECDLPが解ける。ちなみに、点列$\{X_0, X_1, \cdots\}$が上記の図のようにギリシャ文字のρのように点在することから、この手法はρ法と呼ばれている。

次にECDLPに対するρ法攻撃アルゴリズムを以下に示す：

**Algorithm 3** $\rho$法攻撃アルゴリズム

**Require:** 素数位数$r$の点$S \in E(\mathbb{F}_p)$, $T \in \langle S \rangle$.

**Ensure:** $T = dS$を満たす整数$d$.

1: ランダムに整数$u_0, v_0$を選び、初期点を$X_0 = u_0 S + v_0 T$とおく。

2: 点$X_{i+1} = f(X_i)$を順に計算し、衝突が起きるまで繰り返す。

3: 衝突$X_i = X_j$が起きた場合、$v_i \equiv v_j \bmod r$のときステップ1に戻る。それ以外のとき、$d \equiv \frac{u_i - u_j}{v_j - v_i} \bmod r$を満たす整数$d$を見つける。

4: 整数$d$を出力する。

注 3.5. 衝突が起こるまでに必要な点列$\{X_0, X_1, \cdots\}$の個数の期待値は誕生日の逆理（birthday paradox）より

$$\sqrt{\frac{\pi r}{2}} \approx 1.2533\sqrt{r}$$

であることが知られている。よって、$\rho$法を用いてECDLPを解くのにかかる時間の期待値は

$$\sqrt{\frac{\pi r}{2}} \cdot t(f)$$

となる。ただし、$t(f)$は写像$f$を計算するのにかかる時間とする。また、$\rho$法は並列化することができ、$M$台の計算機を用いれば一台の計算機で行うよりも$M$倍高速化することができる。

# 4 楕円曲線暗号の安全性

ECDLPに対する代表的な攻撃法について以下でまとめておく（*については上記で説明していない）：

| 攻撃 | 説明 |
|---|---|
| MOV攻撃 | ECDLPを群$\mathbb{F}_{p^m}^{\times}$の離散対数問題に帰着。埋め込み次数$m$が小さいとき有効。（$E$:supersingular ⇒有効） |
| SSSA攻撃 | Anomalous楕円曲線のとき多項式時間で解読可能。 |
| $\rho$法 | 一般のECDLPに対し現在最も効率がよい。 |
| Index-Calculus法* (Xedni-Calculus法) | 有限体のECDLPを有理数体に持ち上げる方法[7]。効率的でないことが既に知られている[8]。 |
| BSGS法* | 一般のDLPを解く方法[1]。 |
| Weil-descent法* | 標数2上のECDLPに対して有効。ある曲線のヤコビアン群に帰着[3]。 |

$\rho$ 法を用いて ECDLP を攻撃したときにかかる計算時間について説明する。通常楕円曲線暗号で使用されるパラメータサイズは 160 ビットなので、$p \approx r \approx 2^{160}$ とする。また $t(f) = 10^{-5}$ 秒と仮定すると、ECDLP を解くのにかかる計算時間は

$$1.2533 \cdot 2^{80} \cdot 10^{-5}\text{秒} = \text{約}\, 1.3 \cdot 10^{23}\text{年}$$

と見積もれる。これにより、複数台の計算機を用いても現実的な時間では解読できないことが分かる。

ECDLP の解読に関する最新結果について以下でまとめておく：

(i) Certicom 社の ECC challenge については、Texas Tech 大学の Chris Monico 助教授の研究チームが 2002 年に 109 ビットの ECDLP である ECCp-109 を約 10,000 台の計算機を用い、549 日かけて解いた。また、同研究チームは 2004 年に標数 2 の体上の ECDLP である ECC2-109 を約 2600 台の計算機を用い、17ヶ月をかけて解いた。ちなみに過去に解かれた ECDLP はすべて $\rho$ 法を用いて解読されている。

(ii) 2009 年 7 月に ECC challenge 問題ではないが 112 ビットの ECDLP である ECC-P112 が解読された。解読に要した期間は 2009 年 1 月 13 日から 2009 年 7 月 8 日の約半年間で、約 200 台の Play Station 3(PS3) を利用したと報告されている。(詳細：`http://lacal.epfl.ch/page81774.html`)

# 5 $p$ 進数体 $\mathbb{Q}_p$ 上の ECDLP

ここでは、以下の $p$ 進数体 $\mathbb{Q}_p$ 上の楕円曲線に対する ECDLP を考える（今のところ、楕円曲線暗号の安全性とは無関係な問題）：

**$\mathbb{Q}_p$ 上の ECDLP**

$p > 3$ を素数とし、$\mathbb{Q}_p$ 上の楕円曲線

$$\widetilde{E} : y^2 = x^3 + ax + b \ (a, b \in \mathbb{Z}_p)$$

を考える。簡単のため、$\widetilde{E}$ の還元曲線 $E$ は非特異と仮定する。無限位数の楕円曲線の点 $S = (x_S, y_S)$ を固定し、$T = (x_T, y_T) \in \langle S \rangle$ とする。このとき、$T = dS$ を満たす整数 $d$ を見つけよ。

点 $S$ の位数が無限であるため、$\rho$ 法による攻撃が不可能であることに注意する。ここでは、$\mathbb{Q}_p$ 上の ECDLP を解く 1 つの方法を以下で説明する。

SSSA 攻撃と同じように 2 つの関係式

$$0 \to \ker \pi \to \widetilde{E}(\mathbb{Q}_p) \xrightarrow{\pi} E(\mathbb{F}_p) \to 0$$

$$\ker \pi \simeq \mathcal{E}(p\mathbb{Z}_p) = p\mathbb{Z}_p$$

を考える。さらに、$\mathbb{Q}_p$ 上の ECDLP を解くために、次の filtration を考える：

$$\mathcal{E}(p\mathbb{Z}_p) \supset \mathcal{E}(p^2\mathbb{Z}_p) \supset \mathcal{E}(p^3\mathbb{Z}_p) \supset \cdots.$$

この filtration には、同型

$$\mathcal{E}(p^n\mathbb{Z}_p)/\mathcal{E}(p^{n+1}\mathbb{Z}_p) \simeq \mathbb{F}_p, \quad \forall n \geq 1$$

が存在する。有限体 $\mathbb{F}_p$ 上の楕円曲線 $E$ に対して、$N = \sharp E(\mathbb{F}_p)$ とおく。合成写像

$$h : \widetilde{E}(\mathbb{Q}_p) \xrightarrow{N} \ker \pi \simeq p\mathbb{Z}_p$$

を考える。点 $P \in E(\mathbb{Q}_p)$ に対して、

$$h(P) = -\frac{x}{y}, \quad NP = (x, y) \in \ker \pi$$

となる。合成写像 $h$ と上記の性質を組み合わせて、以下のアルゴリズムを考える [9]：

**Algorithm 4** $\mathbb{Q}_p$ 上の ECDLP 攻撃アルゴリズム

**Require:** 無限位数の点 $S \in \widetilde{E}(\mathbb{Q}_p)$, $T \in \langle S \rangle$.
**Ensure:** $T = dS$ を満たす整数 $d$.

1: $N \leftarrow \sharp E(\mathbb{F}_p)$.
2: $NS = (x, y)$ を計算し、$a = -\frac{x}{py} \bmod p$ をおく。(簡単のため、$a \not\equiv 0 \bmod p$ を仮定。)
3: $n = 0, \ell = 1, S' = S, T' = T$ とおく。
4: **while** $T' \neq 0$ **do**
5: $\quad NT' = (x, y)$ を計算し、$w = -\frac{x}{y}$ とおく。
6: $\quad b = \frac{w}{p^\ell}$ とおく。
7: $\quad d_n = b \cdot a^{-1} \bmod p$ かつ $0 \leq d_n \leq p - 1$ を満たす $d_n$ を求める。
8: $\quad T' \leftarrow T' - d_n S', S' \leftarrow pS'$.
9: $\quad n \leftarrow n + 1, \ell \leftarrow \ell + 1$.
10: **end while**
11: $d = \sum_{i=0}^{n-1} d_i p^i$ を計算。
12: 整数 $d$ を出力する。

例. $p = 547$, $\widetilde{E} : y^2 = x^3 + 3x$, $S = (x_S, y_S)$, $T = (x_T, y_T)$

$$\begin{cases} x_S = & 137 + 410p + 136p^2 + 410p^3 + 136p^4 + O(p^5), \\ y_S = & 341 + 478p + 341p^2 + 478p^3 + 341p^4 + O(p^5), \\ x_T = & 97 + 358p + 346p^2 + 320p^3 + 323p^4 + O(p^5), \\ y_T = & 47 + 512p + 514p^2 + 409p^3 + 431p^4 + O(p^5). \end{cases}$$

とおく。上記のアルゴリズムを用いると、$d_0 = 508,\ d_1 = 46,\ d_2 = 1$ を得る。よって、

$$d = d_0 + d_1 p + d_2 p^2 = 324879$$

が得られる。

例から分かるように、上記のアルゴリズムは解 $d$ に対する $p$ 進展開

$$d = \sum_{i=1}^{n-1} d_i p^i$$

を与えることが分かる。また $d < 0$ のときは、上記のアルゴリズムは有限回では終わらないことに注意しておく。

## 謝辞

本講演の機会を与えてくださった金沢工業大学・情報学部竹島卓教授、富士通研究所下山武司主任研究員に感謝する。また、本資料の一部をまとめてくれた九州大学数理学府グローバル COE 研究員安田貴徳氏に感謝する。

## 参考文献

[1] I. Blake, G. Seroussi and N. Smart, Elliptic Curves in Cryptography, Cambridge University Press (1999).

[2] Certicom, Curves List, available at `http://www.certicom.jp/index.php/curves-list`.

[3] H. Cohen and G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Mathematics and Its Applications **34** (2005).

[4] D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer Professional Computing (2004).

[5] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," IEEE Transactions to Information Theory **39** (1993), pp.1639-1646.

[6] T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves," Comm. Math. Univ Sancti Pauli **47** (1998), pp.81-92.

[7] J. H. Silverman, "The Xedni Calculus and the Elliptic Curve Discrete Logarithm Problem," Designes, Codes and Cryptography **20** (2000), pp. 5-40.

[8] J. H. Silverman and J. Suzuki, "Elliptic curve discrete logarithms and the index calculus," Advances in Cryptography - ASIACRYPT '98 (Lecture Notes in Computer Science. vol. 1514), Springer-Verlag, 1998, pp. 110-125.

[9] M. Yasuda, "The discrete logarithm problem on elliptic curves defined over $\mathbb{Q}$," available at `http://portal.acm.org/citation.cfm?id=1394074`.